

July 26, 2012

Federal Communications Commission
Office of the Secretary
Room TW-A325
445 12th Street SW
Washington, DC 20554

Re: CC Docket No. 96-115-Privacy and Security of Information Stored on Mobile
Communications Devices

To Whom it May Concern:

The Consumer Bankers Association (CBA)¹ appreciates the opportunity to submit comments to the Federal Communications Commission (FCC) in response to its recent request for information regarding the privacy and data security practices of mobile wireless service providers. Specifically, the request is for input regarding customer information stored on mobile communications devices, as well as the application of existing privacy and security requirements for that information.

The FCC solicited similar input five years ago, and we agree with the FCC that the technologies associated with these devices have become significantly more sophisticated and powerful since then and that another review of these issues is warranted. Banks have also become much more involved over the past five years in providing their customers with access to banking and payment services by way of mobile devices. As has always been the case, security and privacy are major concerns for banks in a mobile or other type of environment.

However, the mobile environment differs somewhat from others in that it is increasingly complicated and dependent on different types of parties, such as wireless service providers, mobile device manufacturers, and those who develop and construct the mobile applications and operating systems used in these devices. In addition, new entities have entered and continue to enter this relatively new and growing market. Given this type of environment and the various entities involved, we believe all of these involved parties have the responsibility coordinate and ensure consumers have sufficient privacy and security protections. Otherwise, innovation in this area could be stifled.

One issue with regard to this shared responsibility is the extent mobile wireless service providers should be required to erase data from these devices when requested to do so by the customer. These devices may contain a large amount of private and sensitive information, including a

¹ The Consumer Bankers Association ("CBA") is the only national financial trade group focused exclusively on retail banking and personal financial services — banking services geared toward consumers and small businesses. As the recognized voice on retail banking issues, CBA provides leadership, education, research, and federal representation for its members. CBA members include the nation's largest bank holding companies as well as regional and super-community banks that collectively hold two-thirds of the total assets of depository institutions.

significant amount of financial information that will continue to grow as mobile banking and payment services become more prevalent in the future. It is, therefore, critical that providers assume the responsibility to erase this information and to disable the SIM card if the customer requests this be done, such as when the mobile device is lost or stolen.

We also believe these service providers should have responsibilities for ensuring that mobile applications do not contain malware or are otherwise compromised. We encourage the FCC to carefully review this issue to determine the extent providers should bear this responsibility.

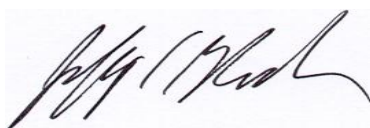
In general, the banking industry would benefit by more information as to the data collected by the wireless service providers and the extent this is shared with third parties. This will be important in the future as mobile banking and payment services become more widespread and will also help banks comply with their privacy and security obligations, such as those with regard to breach notifications. We encourage the FCC to review these information collection and sharing practices as part of this review process.

The issue of breach notifications is of particular concern to financial service providers, merchants, and other industries that have the responsibility of protecting sensitive information. However, this should also be of significant concern to all parties involved in mobile communications in that data breaches are high profile incidents that receive significant press coverage. This not only affects the reputation of the specific parties involved, but may at some point affect the extent newer financial services are adopted by consumers, such as mobile banking and payments, in which consumers may not be as familiar with the privacy and security safeguards that are in place for these specific services. This would adversely affect all parties involved in providing mobile communications if this ultimately leads to consumers reducing the overall use of their mobile devices.

On a related issue, we note that storing information remotely, or “in the cloud,” has become increasingly popular in recent years. Although we expect further refinements and improvements in the future, one benefit of storing information in this manner is that security can be improved under such a process in which information is retrieved pursuant to an authenticated request from the consumer, as opposed to storing sensitive information on the mobile device. We encourage the FCC to further study this issue of security as it applies to storing information “in the cloud.”

Thank you for the opportunity to comment on these issues with regard to privacy and security of information stored on mobile devices. If you have any questions or wish to discuss these issues further, please feel free to contact me at (202) 255-6366 or at jbloch@cbanet.org.

Sincerely,

A handwritten signature in black ink, appearing to read 'Jeff P. Bloch', is written over a light blue rectangular background.

Jeffrey P. Bloch
Associate General Counsel